Secure Online Voting System

Sanam Mijar and Pramod Parajuli

March 14, 2020

Secure Online Voting System

Sanam Mijar[1], Pramod Parajuli[2]

Abstract

Voting is one of the most important activities to build consensus among people, groups, systems, etc. Primitive operations of voting such as the nomination of a candidate, selection of a candidate, casting a vote and counting are easily implemented in a computerized voting system. However, the privacy of voters and their votes plays the most important role in voting. Lack of privacy in voting systems results in balking out from the voting process (Kiayias et al., 2006). Due to ease of access to data and instant sharing capabilities in digital systems, many voters do not feel comfortable using online voting systems. Due to the sheer increase in the use of smartphones, voters also prefer to cast their votes via mobile devices. This paper presents a privacy-aware and security-enforced online voting system platform that is built using an Android mobile app and a secure server that maintains the privacy of voters and their votes. Security measures such as SHA3-512, AES encryption, and JSON Web Tokens for security are used. These measures reduce the risk of man-in-the-middle attacks and accidental/intentional data breach. For end user's ease of use, fingerprint data using FP standards are used for 2-Factor Authentication (2FA). A three-tier (3-tier) architecture is developed to build a voting API, database server with data anonymity, and Android app for a client device.

Keywords: *AES, Android, session security, SHA3-512, voting*

1. Introduction

1.1. Background

Voting is a very important activity to build consensus and deliver an opinion in mass. Similarly, in elections, citizens don't vote for making any political parties just to win and take a leading position, citizens set hope for good and sustainable development in the country by electing a good leader who can understand the need of the country and its citizens. Estonia was the first to use the online voting system. The electronic voting

[1] *Bachelors in Information technology (BIT) Padmashree International College, Nepal*

[2] *Supervisor, Padmashree International College, Nepal*

system is getting popular lately in most countries. When voting is performed online, the voter’s information needs to be protected from information misuse. Voting is important not only for national elections but also it is very useful in various sectors like colleges, schools, offices, etc. for selecting a different person for a different post.

Secure Online Voting System is an electronic platform for casting the vote to the elected candidate that uses a Secure Hash Algorithm (SHA3-512) to hash voter’s information and their voting preferences. The proposed system allows electoral to create a different poll for different purposes such as a poll for a national election, a poll for any school/college/office election. It makes the voting process easy, portable, very convenient and more importantly secure and private so that any eligible voters can vote from anywhere in the world. As the proposed system is a network-based application so, it requires an active internet connection to work.

1.2. Problem Statement

In an online voting system, some researchers found to have potential security flaws and this has made an online election process vulnerable (Schwartz, 2018). In-state elections in Australia, researchers from the University of Melbourne have demonstrated massive security flaws in state elections (Porup, 2018). One of the drawbacks of using an online voting system is that no one can even know if the vote result were manipulated. In the internet world, the online voting system is easier to attack than other online services like online banking. Attackers use various techniques like man-in-the-middle attacks to obtain/modify users’ information. Thus, the use of an appropriate hashing algorithm confirms the integrity of data.

2. Literature Review

There has already been lots of researches and applications made for an online voting system for various platforms. Online voting is the process of voting through an electronic medium mainly by the use of the Internet. Hashing algorithms are mostly used to mask a complex password or any information. In voting systems, voter validation is performed by matching voter's detail information, confirming voter’s id, verifying email, phone or SMS, verifying Irish, fingerprint, etc.

There are lots of hashing algorithms available including MD5, SHA-1, SHA-256, SHA-512, SHA-3 (Keccak), RipeMD-160, Whirlpool, scrypt(N=8192, r=8, p=1), bcrypt (4 or 12 rounds), and many more. Algorithms like MD5, SHA-1, SHA-256, etc. are not secure anymore due to short size hash and high chances of hash collisions (Strauss, 2017).

Message Digest 5 (MD5) is a cryptographic function that accepts input of any random length and produces a message digest of 128-bit length which is known as the hash. It was designed by Ronald Rivest in 1991. This method is fast so it is used in comparing long messages quickly.

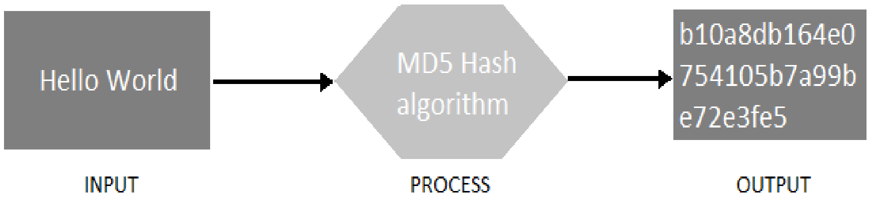


Figure 1: MD5 hashing process

Nowadays, the MD5 method of hashing is not secure enough to protect data as 128-bit hash has probabilities of hash collisions and chances of reverting to original data if the data is small in size.

Another approach is the SHA-256 hash encryption algorithm that uses a 256-bit key length to hash the data for storing voter information in the database.

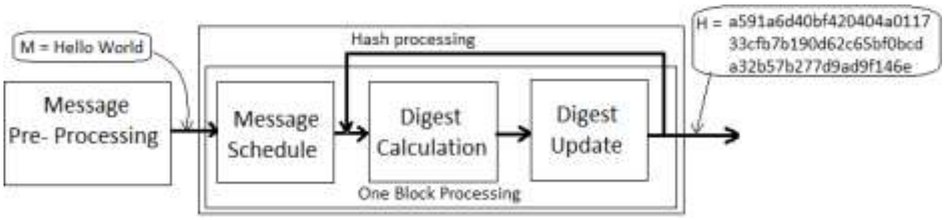


Figure 2: SHA256 hashing process

This method of the hash mechanism is also considered to be vulnerable and not secure enough in current days to make users data secure. SHA-512 algorithm uses multiple rounds to generate hash values and hence considered to be more secure than its predecessors.

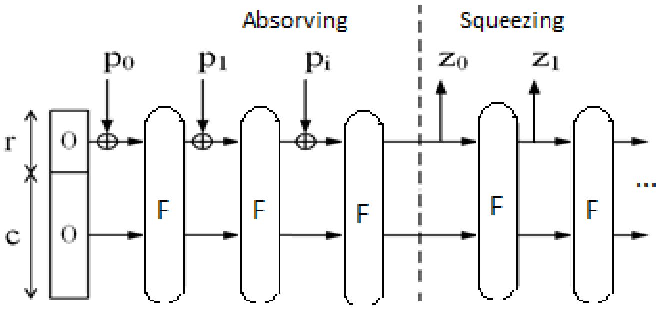


Figure 3: SHA3-512 hashing process

Although the SHA3-512 is part of the same series of standards, it works differently in the hashing process than its other family members like MD5, SHA-1, and SHA-2. It is designed by (Guido et al., 2015). It is based on the novel approach called sponge construction which is based on a wide random function or random permutation whereas the user input is known as "absorbing" and output as "squeezing" in terms of sponge terminology. Due to this technique of hashing, it provides greater flexibility.

Table 1: NIST standard for SHA3 algorithm

Hash		**Output size (bits)**	**Block size (bits)**	**Rounds**	**Operations**	**collision**
SHA-3	SHA3-224	224	1152	24	Keccak[448](*M* || 01, 224)	112
	SHA3-256	256	1088	24	Keccak[512](*M* || 01, 256)	128
	SHA3-384	384	832	242	Keccak[768](*M* || 01, 384)	192
	SHA3-512	512	576	24	Keccak[1024](*M* || 01, 512)	256

Estonia was the first country to use Internet voting and still, more than 30% of ballots are cast online. In the system, the security system was based on a combination of in-person election observation, code review, and adversarial testing. The voter's special client software and national ID smart cards were used to make the vote and for the verification process they use a smartphone app that helps voters to confirm their vote being recorded successfully. The voting process in the system used public-key cryptography that provides the digital analog of the "double envelop" which often used for absentee voting. The first/outer envelope uses a digital signature for the voter identification whereas the second/inner envelop uses cryptographic public encryption key for protecting the ballot. The system adopted a model that consists of various threats and is considered as the radical intimidation that a national election system has faced. This intimidation also includes the fraudulent insiders as well as state-sponsored attacks and also has many serious architectural limitations and loopholes, (Springall et al., 2014).

A new electronic voting system using block-chain technology along with cryptographic techniques to verify resources and to make voters information confidential was developed by Willem et al. (2016). The ballot information is encrypted and the vote is sent to the central block-chain electronic polling station. The encrypted ballot was then decrypted by the centralized authority.

The online voting system by Kadam (2016), is a system made for voters in California to make an online vote for the state elections which is similar to the traditional method of the voting system but instead of using paper ballots it uses an electronic device that takes the digital vote. This online voting system takes voters unique ID input for verification after then the election commission verifies the voter then they will be able to see the bio-data of all candidates. This system managed the voter's data and information through which voters can log in to the system and make their vote using their voting rights. For security measures, facial recognition is used to verify the voter by matching the face registered in the database. After the successful vote election commission evaluates and publishes the result.

The online voting system by Thakkar et al. (2016) is an Android application through which voters can log in to the system providing their voter ID and password as for the security measure for verification in which the voter's information will be checked for matching in the database. And once the information matches or verified from the database, voter now gets the One Time Password (OTP) through their selected medium like SMS or email. The OTP will be encrypted using the play fair cipher algorithm. After all this process of verification and insertion now voters can access the candidate list and then they can give their vote for the preferred ones.

A biometric online voting system is a web-based online voting system that improves the electoral process by providing fast, accurate and secured election results. In this voting system, there will be two different users for the creation of data as admin each with their privileges, one is an administrator and the other is a system user. An administrator creates the logs, inserts the candidate's information, creates voter data, party information and closes the web application when done whereas the system user creates logs, creates voter data, and closes web application only. For the registration of voters, the system accepts the voter's fingerprint for the verification process and if the fingerprint is matched to the database then the system issues the PIN for voter else system will rescan the finger for matching fingerprint is not detected. After getting the PIN voters can give the vote. (Joseph D Enoch & Nne .R. Saturday, 2017).

A practical multi-party computation is an algorithm for a secure distributed online voting system that is built on segregating the election in small groups by using an algorithm multi-party computation algorithm that helps to get a voting result from each group. In this voting system, the system doesn't store any sensitive data and information to the public server. This system architecture can operate by combining with other voting systems so the advantage can be doubled. In this system, the election is divided into multiple groups so that each different group of voters from different locations participate in the election process. For security purposes, this system doesn't use any cryptographic process as it can be used in online voting solely or it can be used to combine with other voting systems. (Juanjo Bermudez, 2016). This system seems to have lots of vulnerable as it doesn't have any security features built on it.

A remote voting scheme is a technique that uses the method of blinded signature to the ballot which makes voting untraceable by anyone else back to the voter, (Michael, Radwin & Klein, 1995). A Mobile Voting System (MVS) proposed by Robinson et al. (2011) operates parallel with existing manual and automated voting systems. This system allows the real voters to cast their vote from anywhere they want using the mobile devices.

In the late 2000 U.S. Presidential elections there appear vulnerable issues and to overcome these issues the Caltech/MIT ballot technology project developed a new reasonable ballot technology. The developed system addressed the problems concerning voting systems, a traveler in an early ballot, elector registration, polling places, ballot instrumentation, ballot security cost and public finance of election, etc. and this resulted into replacement technique and framework "A standard ballot design ("Frogs")" within which generation of votes is performed individually from voting, and therefore the "Frog" forms a permanent audit path. Here in this process, the vote generation machine is often proprietary whereas the voting machines must be ASCII text file and completely verified and authorized for correctness and security. The proposed system finally, provides a collection of short and long-run recommendations on the assorted problems associated with the ballot.

3. Methodology

The system development followed the Waterfall software development life-cycle to develop a complete system and test it. Requirements of the proposed system were gathered from various literature reviews on the online voting system. The design of data, workflows, user interface flow of events were determined by analyzing data requirements and end-user workflow. Features expected by administrative users and voters were implemented in PHP and Android platform respectively. Various libraries for implementing hash algorithms were used. Finally, sample data were used to conduct experiments and end-user testing.

4. Implementation model

The proposed secure online voting system uses a SHA3-512 hashing algorithm to make voters information safe and secure along with Two Factor Authentication (2FA) that includes fingerprint verification and One Time Password verification (OTP) to make account accessible to genuine users only.

The proposed system is an Internet-based system that requires Internet access to run. And as it is an Android-based application, the followings show the hardware and software requirements for the proposed system.

For the system, end-users require an android mobile device whereas, for administration, a PC with capabilities to run light-weight server-side services and database servers is more than sufficient.

The proposed system has the following features.

- **Validating Voters:** Anyone in the entire world can install this application but only those who have the valid voter’s information given by the country/school/college/office for each respective election those voters are only allowed to make vote using this system. For example: to make a vote in a national election, voters need to verify by providing their valid citizenship information. In the same way ID card information is required to vote in an election of school/college/office.

These following requirements are fulfilled in the system as it is most essential in the online voting system:

- **Voters Privacy:** All voter information is hashed using the SHA3-512-bit hashing algorithm then only the hashed information is stored in the election database. This helps to keep the voter’s information anonymous.

- **Detection of Multiple vote attempts:** The system allows voters to vote only once in any election. Multiple vote attempts by the same voters are not allowed.
- **Voters vote information privacy:** One the voter makes the vote, no information related to the voter is stored in the vote database. So that no-one knew who has voted for whom.
- **Vote verification:** Once the vote is cast, the system gives voters information of their votes successfully made in case if the vote is successful otherwise the system shows respective error or suggestion for making a vote.

To use the system, initially, users need to create their account in a secure online voting system app then to make a vote using this system, people need their valid identification information according to their preferred election type that includes national election, school/college/office election, etc. To make the voting process more secure, the system needs voters to go through an authentication process which includes fingerprint verification or one-time password (OTP) verification send to their pre-registered phone number in the system. Figure 4 shows the overall voting process using a secure online voting system.

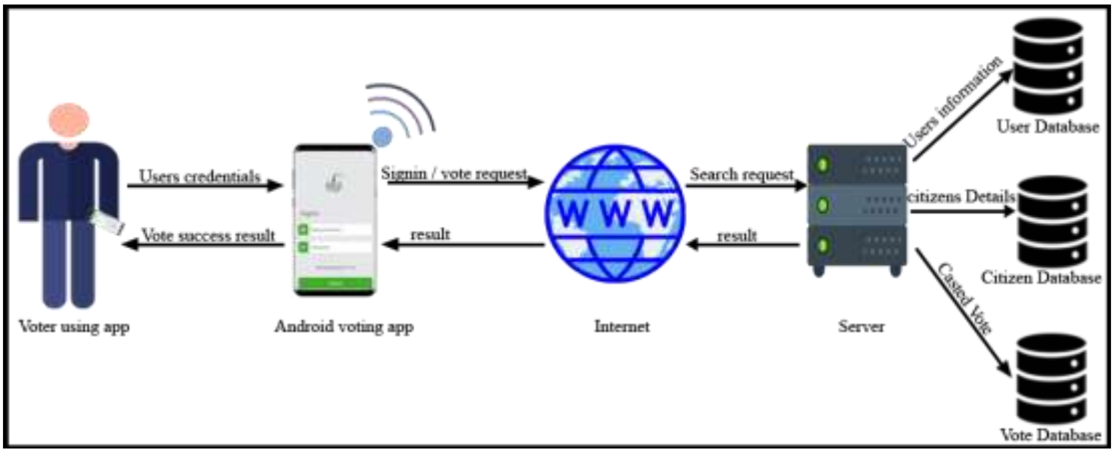


Figure 4: The voting process of secure online voting system

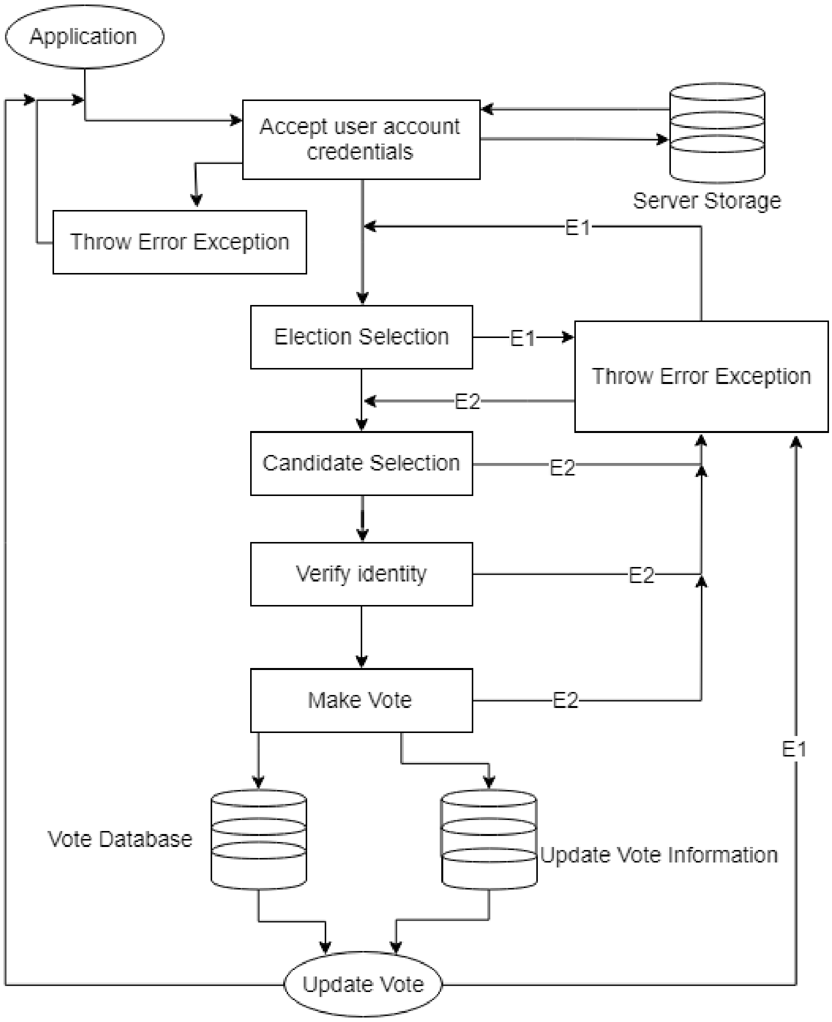
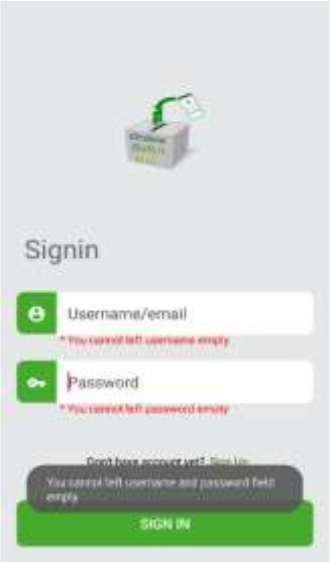


Figure 5: System Implementation

Initially, user signs in the system and there will be two probability correct information or incorrect information, that will be checked from the server and throws error exception in case of error else user selects the election, there system checks for the user if already voted, throws an exception if already voted else user selects the candidate to vote for. If any error occurs while voting, the system throws the exception else vote is updated along with user/voter vote status.

5. Experiments and results

The system is tested many times and as soon as the bugs were found, it is eliminated and solved thoroughly. Initially, the system is tested with empty signs in fields for the user verification process as shown in figure 6. Figure 8 shows the error message when the user tries to sign in to the system with incorrect credentials. While at the requirement analysis phase, whatever requirements were gathered are also tested along with the system design.


Signin

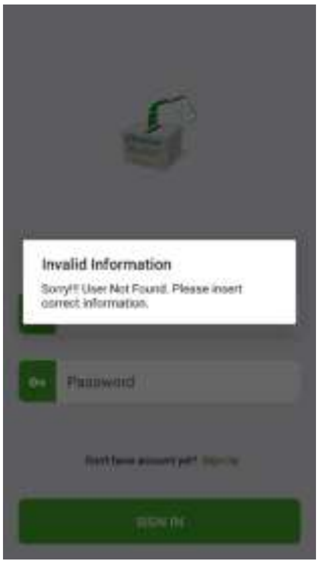
* You cannot left username empty

* You cannot left password empty

Dont have account yet? Sign Up

You cannot left username and password field empty

Figure 6: Error message displaying while pressing the sign-in button with empty fields


Invalid Information

Sorry!!! User Not Found. Please insert correct information.

Don't have account yet? Sign Up

Figure 7: Error message while wrong credential input by the user

For testing the system, many static, as well as dynamic data, were used. Various elections were created along with many voters for each different election. As this system is the voting platform for various elections, a single person can register for more than one election at once. The following table shows the election created by the admin user.

Table 1: Creating different elections

ID	election_id	election_type	election_name	no_of_candidates	election_start_date	election_end_date	election_icon 1
1	4fffa29034a844dfbc74a75b8d17f8e6	National	New Prime Minister Selection	3	2019-09-26 23:20:50	2019-09-30 23:20:50	election icon
2	b307c5ec2f437b3edede3ecfee2eb2cd	College	New College Leader	4	2019-09-21 01:10:20	2019-09-23 01:10:20	election icon
3	75dab1e83d0a290c546764e9fa0751d9	Office	New GM Selection	2	2019-09-29 01:10:20	2019-09-30 01:10:20	election icon

The voter's information is kept secure using the SHA3-512-bit hashing algorithm and to keep voters voting preference un-revealed only voter id and election id is stored in the database which doesn't even reveal whom they have voted. which is shown in the table below:

Table 2: Voters voting preference keeping secure

ID	voter_id	election_id	vote_ status	vote_date
1	23dd9762f5d9593dbb01b5ec61359f53	4fffa29034a844dfbc74a75b8d17f8e6	Voted	2019-09-26 09:44:14
2	23dd9762f5d9593dbb01b5ec61359f53	75dab1e83d0a290c546764e9fa0751d9	Voted	2019-09-27 09:40:40
3	23dd9762f5d9593dbb01b5ec61359f53	b307c5ec2f437b3ededе3ecfee2eb2cd	Voted	2019-09-27 10:34:22
4	ad45925cd47fb82d190499a24b88a573	4fffa29034a844dfbc74a75b8d17f8e6	Voted	2019-09-28 10:44:14
5	e3480a8108a815dcfacfecda86a31889	4fffa29034a844dfbc74a75b8d17f8e6	Voted	2019-09-28 08:43:31
6	b179a9ec0777eae19382c14319872e1b	75dab1e83d0a290c546764e9fa0751d9	Voted	2019-09-28 09:00:15
7	0cb1eb413b8f7cee17701a37a1d74dc3	b307c5ec2f437b3ededе3ecfee2eb2cd	Voted	2019-09-28 10:07:34

The system counts the total votes obtained by each candidate in all different elections and stores in the database. And the final result is shown in the administrator site. The following figures show the number of candidates in all elections and obtained votes of each candidate in each different elections.

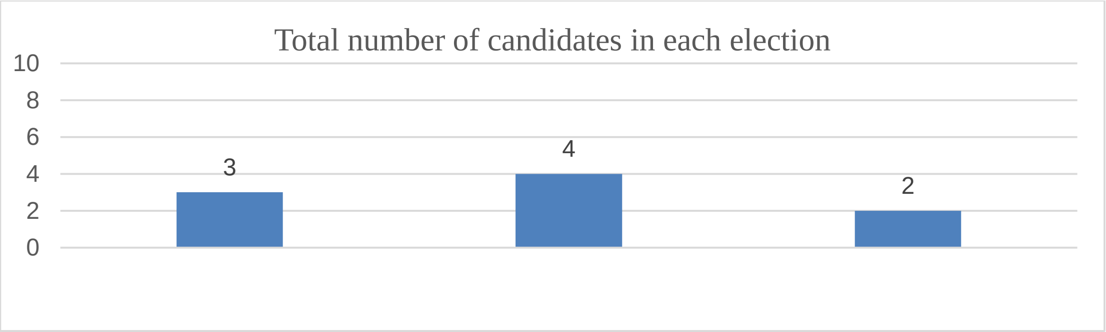


Figure 8: Total number of candidate in all different election

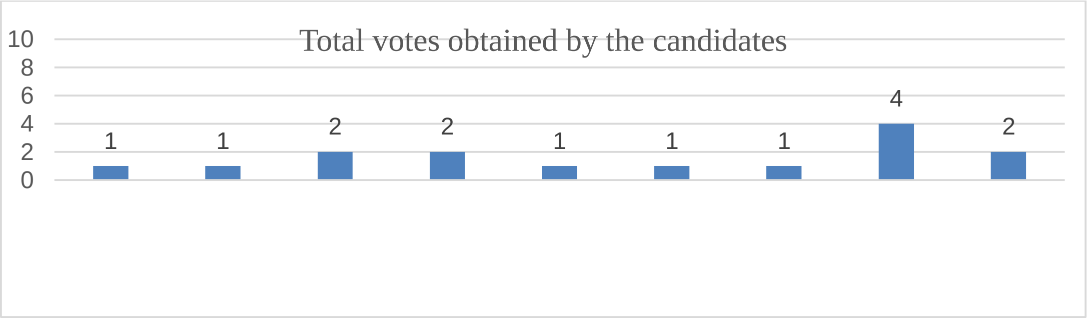


Figure 9: Obtained voted by the candidate in an election

6. Conclusions and Future Work

The proposed system Secure Online Voting System uses the SHA3-512-bit key length hashing algorithm to make voters information secure. Regarding the safety of voters, the anonymity of the voter is maintained so that no information related to voters and their voting preferences is stored in the database. Due to this, the privacy of voters is maintained and the project objective to make voting easy, interactive and secure is done. In the case of the hashing algorithm, SHA3-512 is fast, easy and a little more secure than others in terms of speed of processing. And due to this feature of the SHA3-512 hashing, the proposed system also works completely fine and is appropriate for the system.

There are lots to implement in the system which are not presented at this time. There is another hashing algorithm better than the one discussed in the system but due to its low processing speed, SHA3-512 is used. And if any other fast and more secure methods were available in the future then it is needed to be implemented. Using the current system, user can only create their account and by joining the election they can vote the candidate in an election which is already created by the election officer. So, in the future, the system should provide every user to create their election and add candidates manually themselves as per their needs and requirements.

Besides this, in the proposed system, users are now allowed to see the vote result in real-time, they have to wait for admin users to broadcast the final result but for the future, even the user should be able to see the vote result. The system doesn’t allow a user to modify their vote even if they have voted mistakenly. so in the future, a user should also able to modify the vote and change their votes.

References

Asecuritysite.com. (n.d.). *Spongent*. [online] Available at: https://asecuritysite.com/encryption/spongent [Accessed 14 Sep. 2019].

Baycan, F. (2017). *Şifreleme Algoritmaları - MD5 | Webmaster.Kitchen*. [online] Webmaster.Kitchen - Türkiye'nin Webmaster Mutfağı. Available at: https://webmaster.kitchen/en/sifreleme-algoritmalari-md5/ [Accessed 16 Sep. 2019].

Business-standard.com. (2019). *Online voting technology of Right2Vote is now certified by Government of India*. [online] Available at: https://www.business-standard.com/article/news-ani/online-voting-technology-of-right2vote-is-now-certified-by-government-of-india-119032500520_1.html [Accessed 14 Sep. 2019].

BN, Y. (2018). Electronic Voting System Using Blockchain. [ebook] pp.3 & 8. Available at: https://pdfs.semanticscholar.org/84c7/c5b9df300d5d282038684654e2d47998b3dd.pdf [Accessed 17 Jun. 2019].

D.Enoch, J. and Saturday, N. (2017). Biometric Online Voting System in Nigeria. International Journal of Computer Trends and Technology, 49(1), pp.18-86.

Cryptography Stack Exchange. (2017). *Are there any known collisions for the SHA (1 & 2) family of hash functions?* [online] Available at: https://crypto.stackexchange.com/questions/3049/are-there-any-known-collisions-for-the-sha-1-2-family-of-hash-functions [Accessed 14 Sep. 2019].

Dimple, P. (2014). e-voting system using QR code and Mobile OTP based on Android platform for modern individuals. International Journal of Scientific & Engineering Research, [online] 5(10), pp.1624 - 1628. Available at:

https://pdfs.semanticscholar.org/18b5/49fb6b01062a99474407a09aef55e2a31aef.pdf [Accessed 18 Jun. 2019].

Dwyer, K. (2016). *Cyber Vulnerabilities Threaten 2016 Election - Risk & Insurance*. [online] Risk & Insurance. Available at: https://riskandinsurance.com/cyber-vulnerabilities-threaten-2016-election/ [Accessed 15 Aug. 2019].

Engelfriet, A. (2005). *The MD5 cryptographic hash function (in Technology > hashfunctions @ iusmentis.com)*. [online] Iusmentis.com. Available at: https://www.iusmentis.com/technology/hashfunctions/md5/ [Accessed 12 Sep. 2019].

Harwoeck, F. (2018). *Password and Credential Management in 2018 🔒*. [online] Medium. Available at: https://medium.com/@harwoeck/password-and-credential-management-in-2018-56f43669d588 [Accessed 14 Sep. 2019].

Hassan, S. and Anwar, M. (2018). Voting System using Android Operating System. VAWKUM Transactions on Computer Sciences, 15(1), p.48.

Kadam, T. (2016). Online Voting System. International Journal of Engineering Trends and Technology, 37(5), pp.273-276.

Kiayias, A Korman, M. and Walluck, D. "An Internet Voting System Supporting User Privacy," *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, Miami Beach, FL, 2006, pp. 165-174. [online] Available at: URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4041164&isnumber=4041139 [Accessed 14 Sep. 2019].

May, W. (2015). *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. [ebook] Federal Information Processing Standards Publication. Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf [Accessed 15 Sep. 2019].

M.R, N. (2018). Android Based Voting System for Mobile Device. International Research Journal of Engineering and Technology (IRJET), 05(03), pp.2991 - 2994.

Montco Getting New Paper-Based Voting System. (2018). [image] Available at: https://s.yimg.com/uu/api/res/1.2/gvTFQzkJN.9hVOpVAYhJjA--~B/aD00NTA7dz02MDA7c209MTthcHBpZD15dGFjaHlvbg--/https://cdn20.patchcdn.com/users/22896833/20181214/025155/styles/T600x450/publ ic/processed_images/election-voting_ballot_box_shutterstock_201581045-1544817016-4036.jpg [Accessed 11 Sep. 2019].

Nast, C. (n.d.). *Election Security Is Still Hurting at Every Level*. [online] Wired. Available at: https://www.wired.com/story/election-security-2020/ [Accessed 14 Sep. 2019].

Porup, J. (2018). Online voting is impossible to secure. So why are some governments using it?. [online] CSO Online. Available at: https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html [Accessed 12 Sep. 2019].

Pro, S. (2007). *Project Report On Online Voting System Using Face Recogniton*. [online] Academia. Available at: https://www.academia.edu/6306941/Project_Report_On_Online_Voting_System_Using_Face_Recogniton [Accessed 15 Sep. 2019].

Rouse, M. (2005). What is MD5? - Definition from WhatIs.com. [online] SearchSecurity. Available at: https://searchsecurity.techtarget.com/definition/MD5 [Accessed 12 Sep. 2019].

Schwartz, J. (2018). *The Vulnerabilities of Our Voting Machines*. [online] Scientific American. Available at: https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/ [Accessed 15 Sep. 2019].

Smartsheet. (n.d.). *Waterfall*. [online] Available at: https://www.smartsheet.com/content-center/best-practices/project-management/project-management-guide/waterfall-methodology [Accessed 14 Sep. 2019].

Springall, D.at al Security Analysis of the Estonian Internet Voting System. [ebook] Ann Arbor, MI, U.S.A., pp.1-11. Available at: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf [Accessed 12 Jun. 2019].

STAFFORD, D. (n.d.). digital scan method of voting. [image] Available at: http://s3.amazonaws.com/escambiavotes_com/images/4/original_votehand.jpg?1260375142 [Accessed 11 Sep. 2019].

Strauss, D. (2017). *Stop Using SHA-256*. [online] Medium. Available at: https://medium.com/@davidtstrauss/stop-using-sha-256-6adbb55c608 [Accessed 12 Aug. 2019].

Studymafia.org. (n.d.). *A Seminar report On Online Voting System*. [online] Available at: http://studymafia.org/wp-content/uploads/2015/04/CSE-Online-Voting-System-Report.pdf [Accessed 29 Aug. 2019].

Team Keccak (n.d.). The sponge construction. [image] Available at: https://keccak.team/sponge_duplex.html [Accessed 12 Sep. 2019].

Tutorialspoint.com. (n.d.). *SDLC - Waterfall Model - Tutorialspoint*. [online] Available at: https://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm [Accessed 14 Sep. 2019].

Wong, d. (2017). *SHAKE, cSHAKE and some more bit ordering*. [online] Cryptologie.net. Available at: https://cryptologie.net/article/388/shake-cshake-and-some-more-bit-ordering/ [Accessed 18 Sep. 2019].